HS SEDI
Homeland Security Systems Engineering and Development Institute

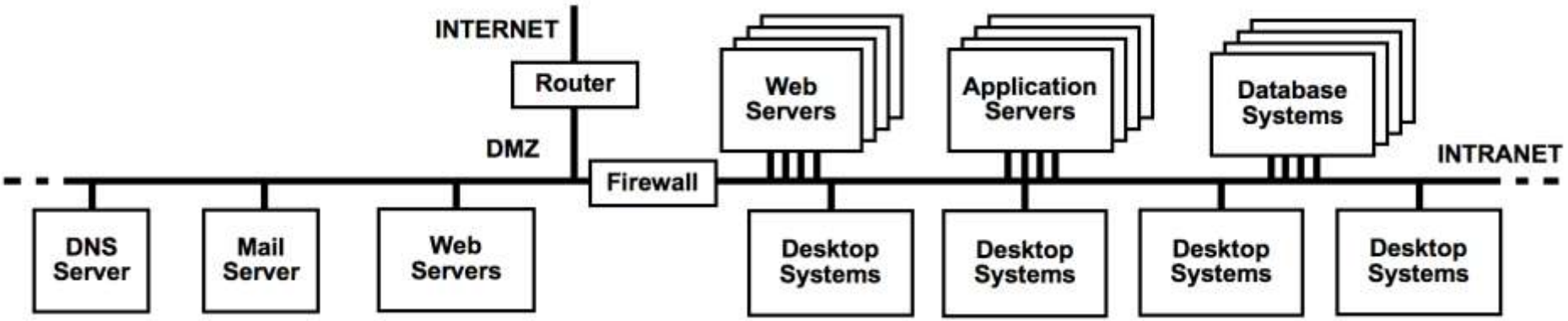
SwA Panel:
Use Cases, Standards and Roadmap for Enterprise Security Automation
-----
Automation Activities for Securing the Enterprise

Robert A. Martin

27 September 2010

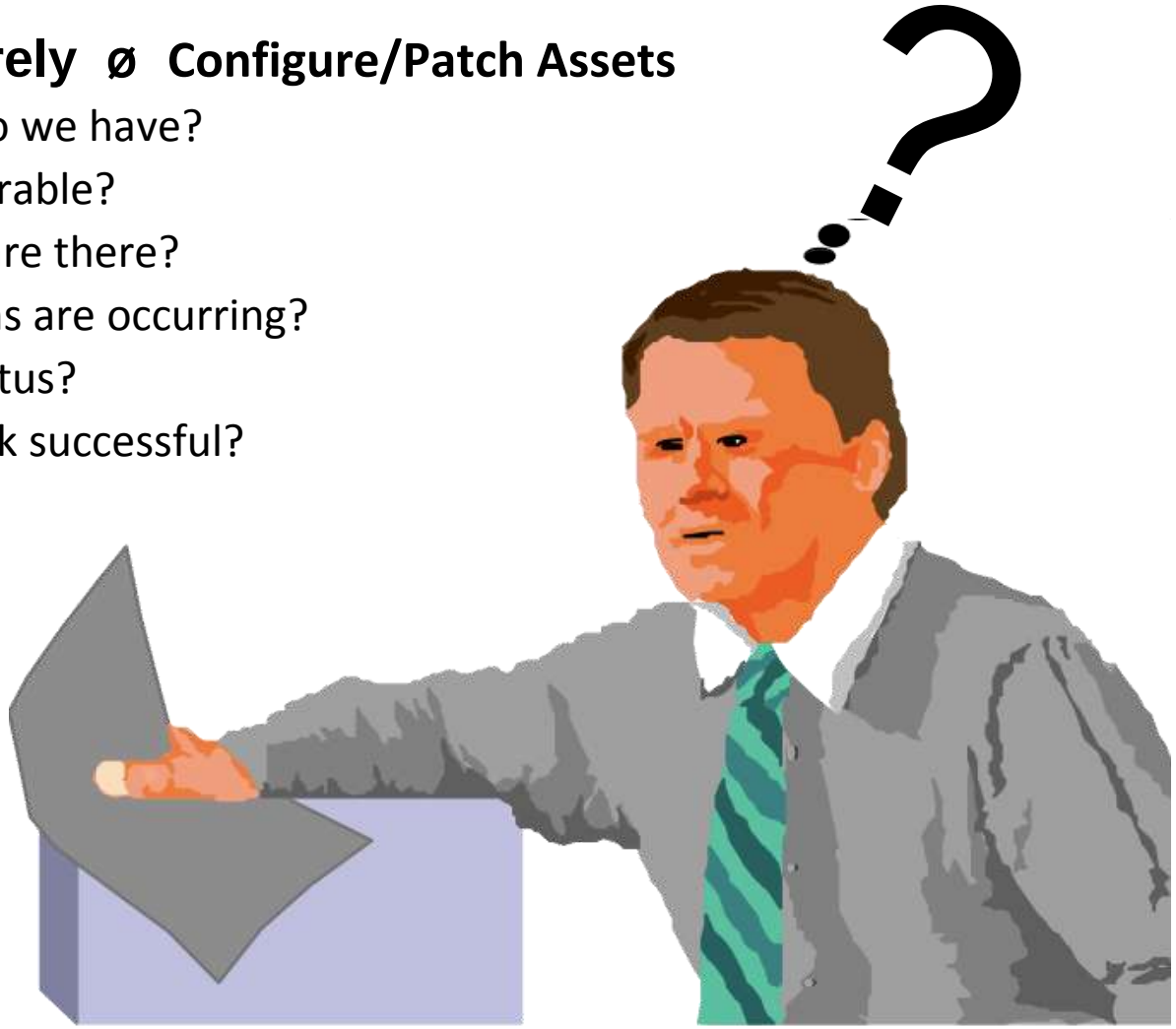
Homeland Security

A Notional Enterprise Information Technology Infrastructure



Securing the Enterprise…

- **Operate Securely ø Configure/Patch Assets**
  - What assets do we have?
  - Are they vulnerable?
  - What threats are there?
  - What intrusions are occurring?
  - What's our status?
  - Was that attack successful?
  - •
  - •
  - •



Cognitive and Cyber Speed Activities & Info (SCAP)

HS SEDI
Homeland Security Systems Engineering and Development Institute

- **CVE identifiers require analysts to investigate/correlate…**
  - Which enables tools to correlate at cyber speed…
- **OVAL definitions require analysts to define criteria…**
  - Which enables checking systems for user defined content at cyber speed…
- **CVSS scores require analysts to assign vector values…**
  - Which enables identifying severity and following a priori guidance on risk tolerance at cyber speed…
- **CPE names require vendors/analysts to assign names…**
  - Which allows correlating platform information at cyber speed…
- **CCE identifiers require analysts/vendors to identify controls…**
  - Which allows correlating settings with desired settings at cyber speed…
- **XCCDF requires analysts to craft policy statements…**
  - Which allows multiple tools to follow and report against user defined content at cyber speed…
- **OCIL requires analysts to craft questionnaires…**
  - Which allows multiple tools to ask and report against user defined content at cyber speed…

SCAP's Automation Requires:

- Consistent input from Cognitive activities feeding SCAP
- Structured input & output to and from those Cognitive activities
- Universal definition of concepts across SCAP elements

Cognitive Speed

Content/Guidance Writing

Enumeration Assignment

Cyber Speed

Assessment by SCAP enabled Tools

Cognitive Speed

Enterprise Security Management

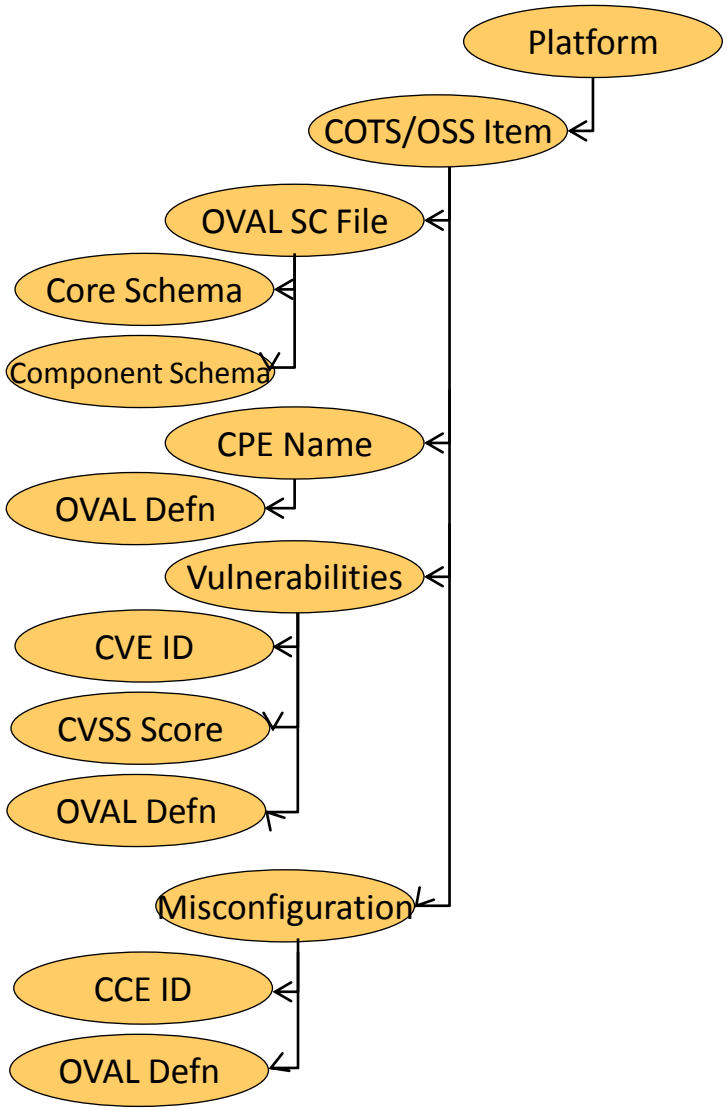
HS SEDI
Homeland Security Systems Engineering and Development Institute

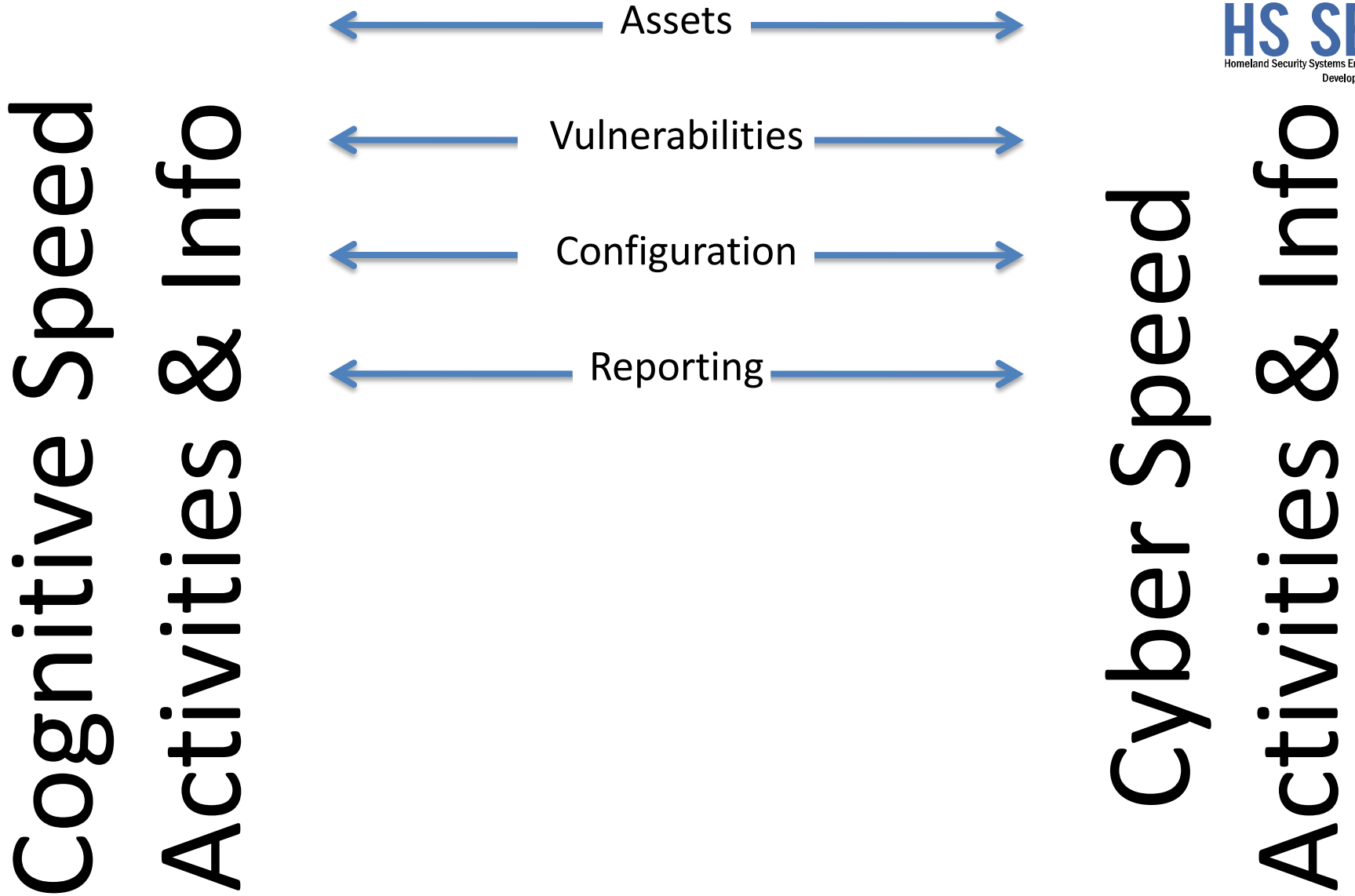
Cognitive Speed Activities & Info

Cyber Speed Activities & Info

SCAP and the model beneath it…

- **A platform:**
  - Commercial or Open Source Software
    - OVAL Systems Characteristics File
      - Core Schema
      - Component Schema
    - CPE names
    - Vulnerabilities
      - CVE identifiers
      - CVSS scores
      - OVAL definitions
    - Misconfigurations
      - CCE identifiers
      - OVAL definitions




Cognitive Speed Activities & Info
Assets
Vulnerabilities
Configuration
Reporting
Cyber Speed Activities & Info

Asset Inventory

Configuration Guidance Analysis

Vulnerability Analysis

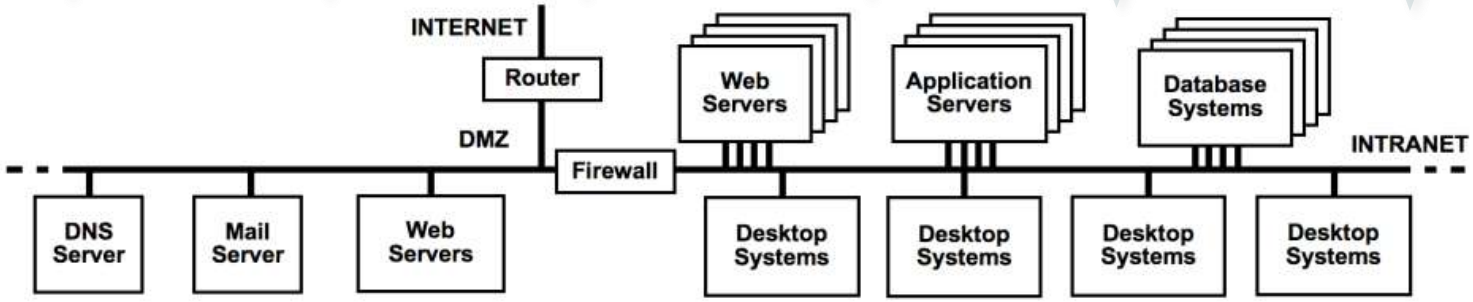
Threat Analysis

Intrusion Detection

Incident Management

Operations Security Management Processes

Assessment of System Development, Integration, & Sustainment Activities and Certification & Accreditation



Operational Enterprise Networks

Development & Sustainment Security Management Processes

Enterprise IT Change Management

Centralized Reporting

Enterprise IT Asset Management

Asset Inventory

Configuration Guidance Analysis

Vulnerability Analysis

Threat Analysis

Intrusion Detection

Incident Management

ESIP

SCAP

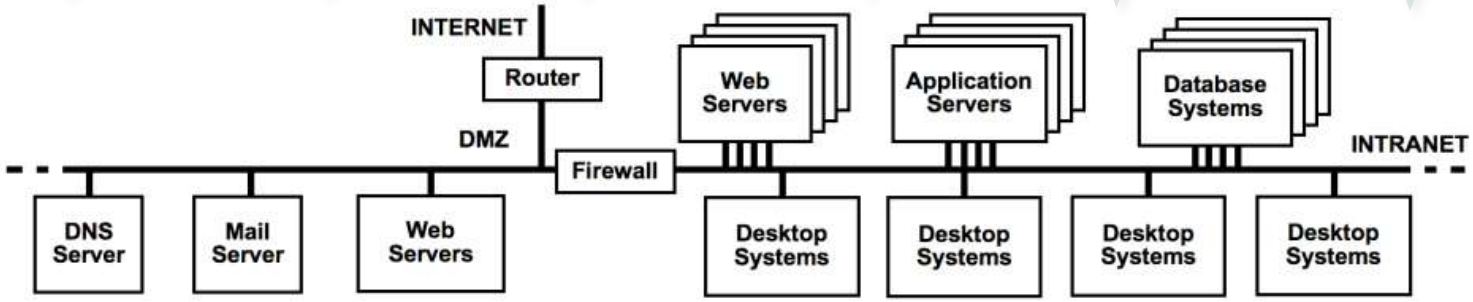
TAAP

EMAP

ITAP

Operations Security Management Processes

Assessment of System Development, Integration, & Sustainment Activities and Certification & Accreditation



SwAAP

Operational Enterprise Networks

ERAP

ECAP

Enterprise IT Change Management

Centralized Reporting

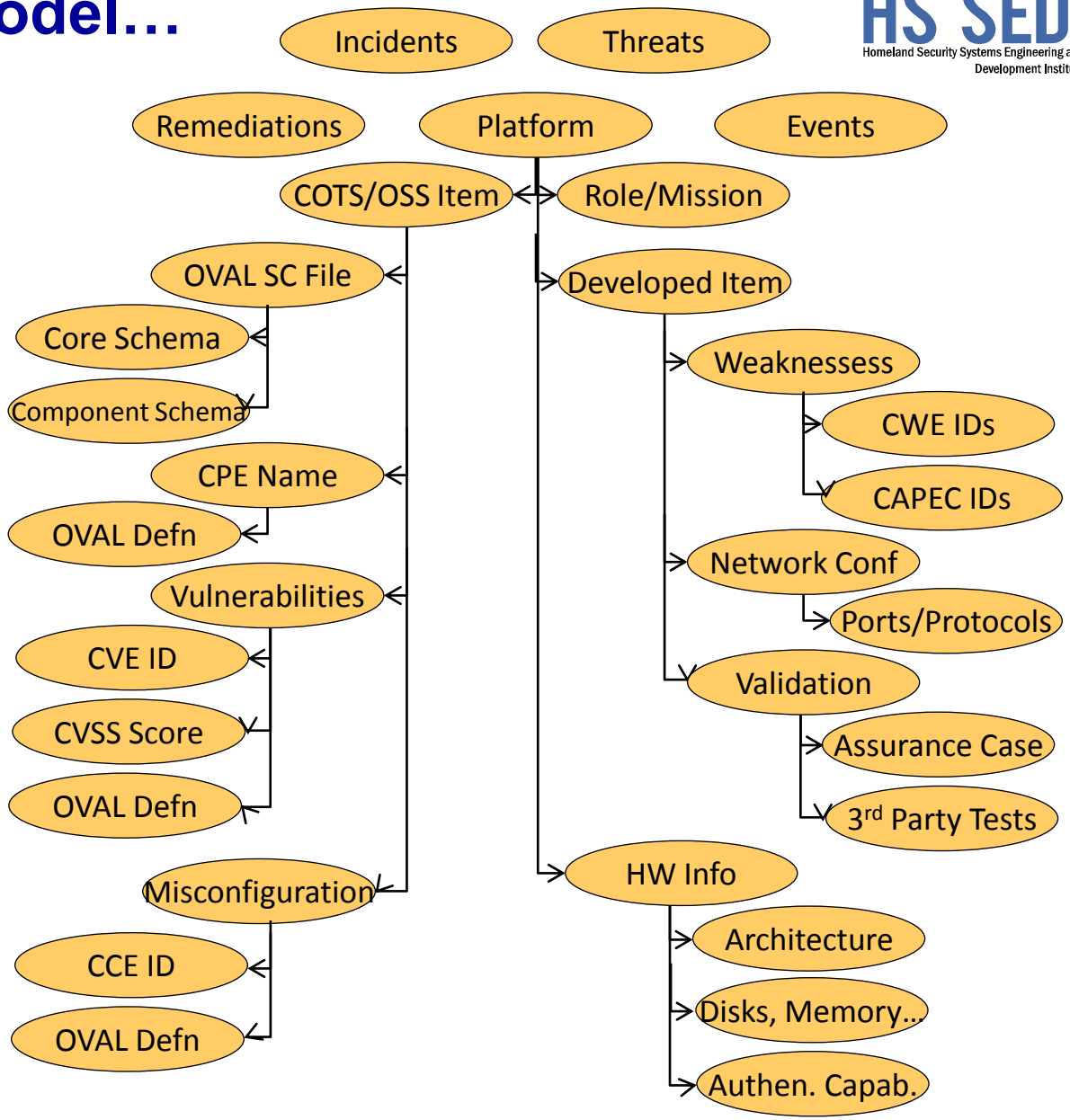
Enterprise IT Asset Management

Development & Sustainment Security Management Processes

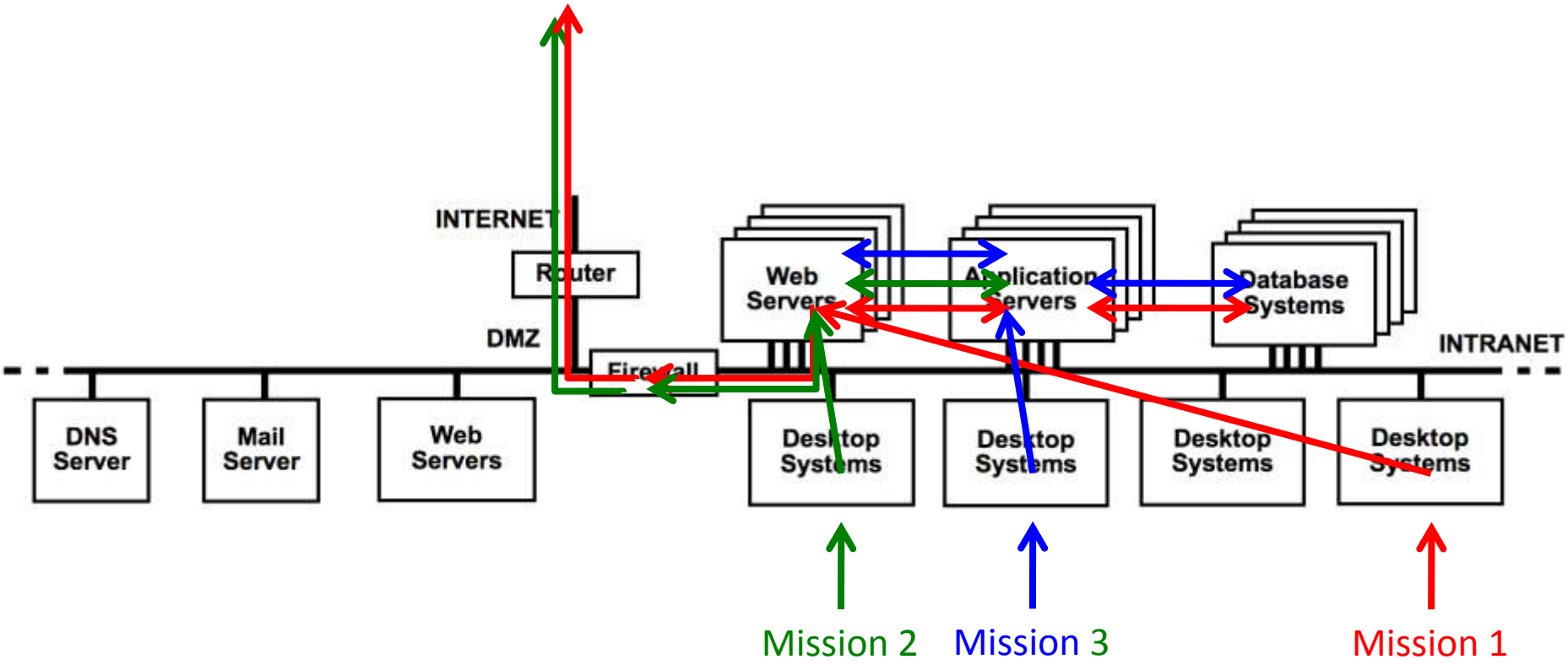
Other things to model…

HS SEDI
Homeland Security Systems Engineering and Development Institute

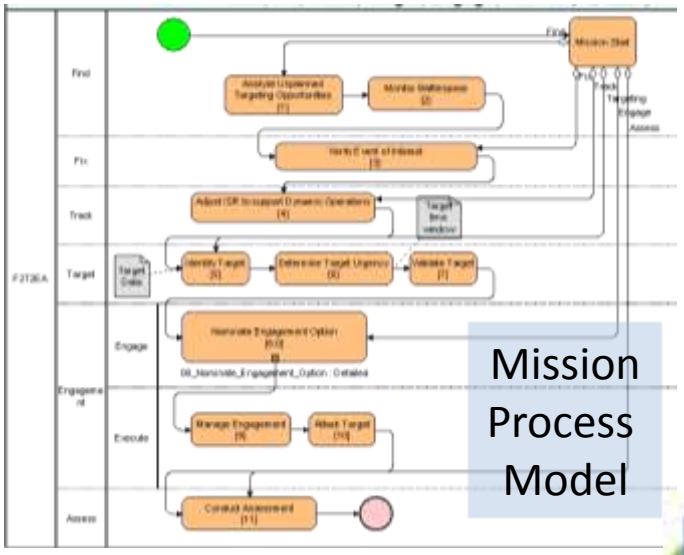
- **A platform:**
  - Role/Mission
  - Hardware Information
    - Architecture
    - Disks, Memory, Comms, Input Devices
    - Authentification Capabilities
  - Organically Developed Software
    - Weaknesses Evaluated For
      - CWE IDs
      - CAPEC IDs
    - Validation Methods
      - Structured Assurance Case
      - 3rd Party Testing
  - Network Configuration Information
    - Ports/Protocols Settings



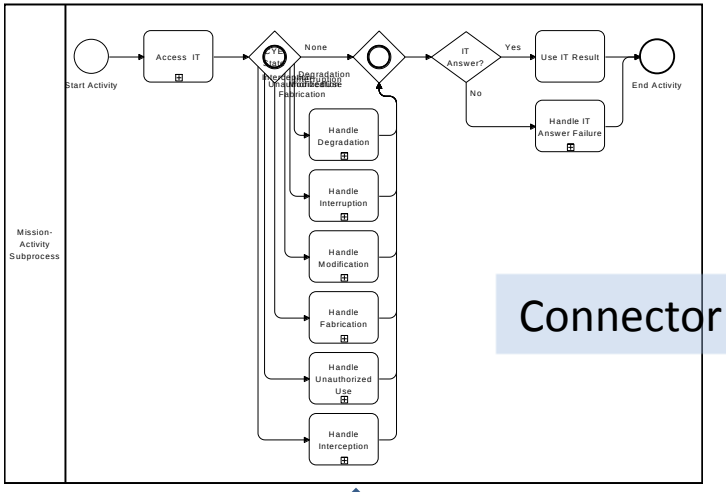
Enterprise Information Technology Infrastructures Are There to Support Missions and Enterprise Capabilities



Mission Modeling: using BPMN (Business Process Modeling Notation) to represent missions and their cyber dependencies

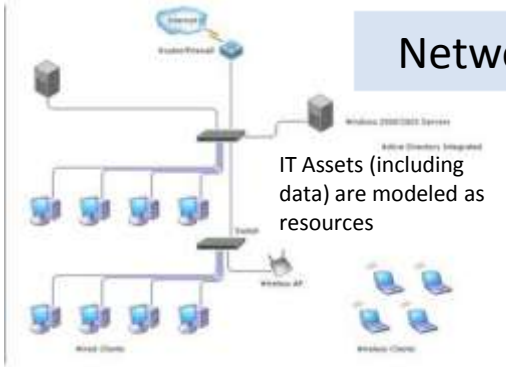


Mission Process Model



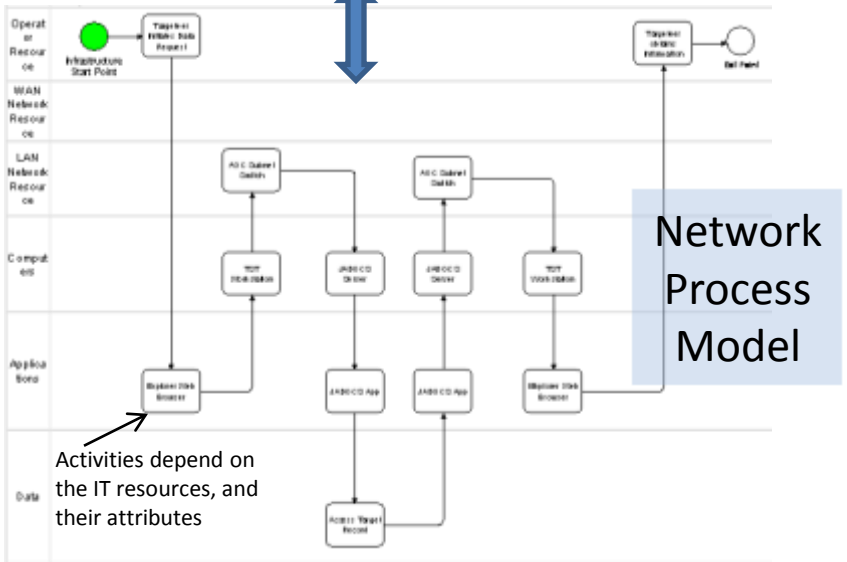
Connector

BPMN



Network Diagram

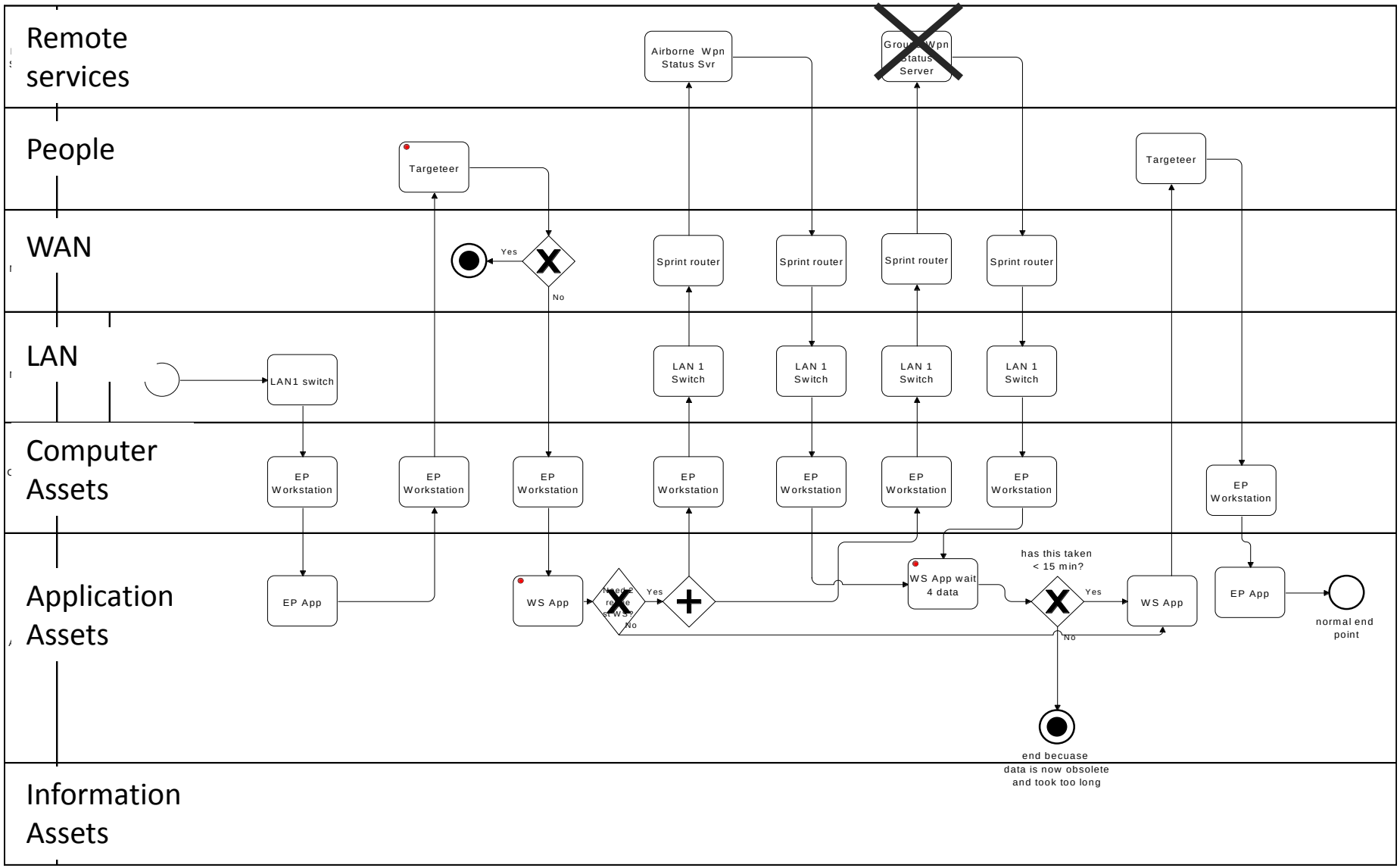
IT Assets (including data) are modeled as resources



Network Process Model

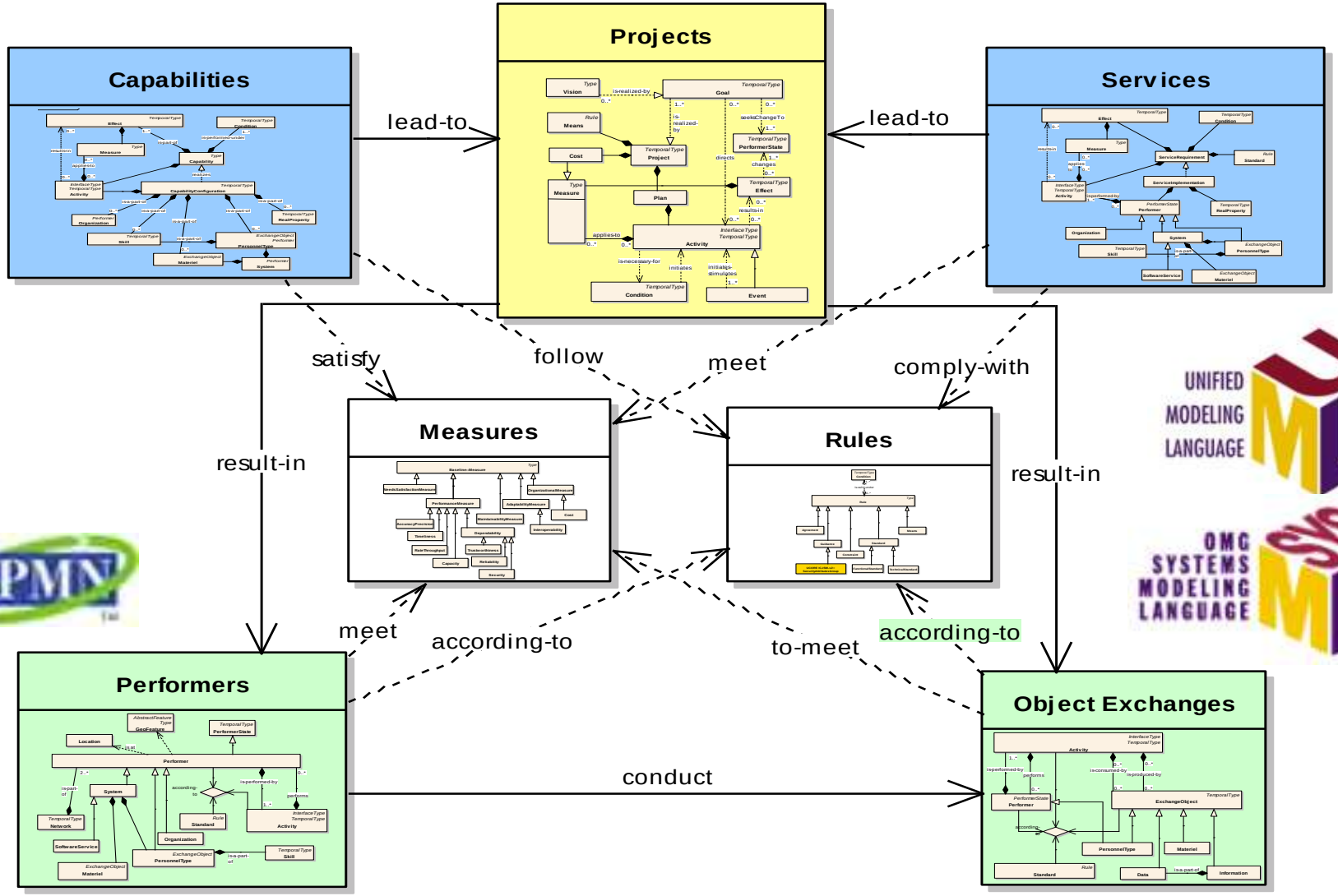
Activities depend on the IT resources, and their attributes

Example Incident: Remote failure interrupts access to a systems status sources



DoDAF Version 2.0 Metamodel

HS SEDI
Homeland Security Systems Engineering and Development Institute



Software Assurance Automation Protocol (SwAAP)

- For measuring & enumerating software weaknesses and the assurance cases.
  - Common Weakness Enumeration (CWE)
  - Common Attack Pattern Enumeration & Classification (CAPEC)
  - Malware Attribute Enumeration & Characterization (MAEC)
  - Common Weakness Scoring System (CWSS)
  - OMG Software Assurance Evidence Metamodel (OMG SAEM)
  - OMG Arguementation Metatmodel (OMG ARG)
  - OMG Structured Assurance Case Metamodel (OMG SACM)
  - Software Assurance Findings Expression Schema (SAFES)
  - NIST SAMATE's "Software Label"
  - OMG Structured Metrics Metamodel (OMG SMM)
  - ISO "Assurance Case" 15026 (ISO 15026)
  - OMG Knowledge Discovery Metamodel (OMG KDM)
  - OMG Abstract Syntax Tree Metamodel (OMG ASTM)

- plus SCAP to capture "accredited" system CPEs and CCE settings?
- OVAL checks for capturing "finger print" of software applications to address supply-chain risk measurement?

HS SEDI
Homeland Security Systems Engineering and Development Institute

Questions Can Be Addressed To:

ramartin@mitre.org

Homeland Security